



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/059,182 | 01/31/2002 | Janne Suuronen | 017.41038X00 | 5357 |

20457 7590 07/26/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

| |
|----------|
| EXAMINER |
|----------|

SHAW, YIN CHEN

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2135

DATE MAILED: 07/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/059,182

Applicant(s)

SUURONEN ET AL.

Examiner

Yin-Chen Shaw

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-55 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-55 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 01/31/02, 04/16/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-55 have been submitted for examination.
2. Claims 1-55 have been examined and rejected.

Claim Interpretation

3. Claims have been afforded their broadest reasonable interpretation. Applicant's language directed to virus is interpreted as equivalent to any code, computer-readable instruction, content, or violation that is intended to cause incorrect and undesirable consequence(s) within computing system. The term "real-time" is interpreted to multimedia data or stream that are associated with video or audio (according to the Microsoft Computer Dictionary, 4th edition). The term "wide area network" is interpreted as equivalent to any networks among the Internet.

Claim Rejections - 35 USC § 112

4. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
 - i. In Claim 1, the phrase recites "a firewall which receives the data packets and virus scanning engine". It is not clear whether the firewall is intended for receiving both the data packets as well as the virus scanning engine. Appropriate correction is required. For examining purpose, the firewall is

considered as intended only for receiving the data packet while the virus scanning engine is used for other functions.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-3, 20-21, 32, 41-45 47, 49-52, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935).

i. Referring to Claim 1:

As per Claim 1, Fink et al. disclose in a communication system including at least a first network [i.e., **external network 14 (Fig. 1)**] coupled to a destination [i.e., **protected nodes 20 in protected network 12 (Fig. 1)**] to which transmissions of data packets are made from the first network to the destination, a system for providing virus protection comprising: a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus [i.e.,

Therefore, according to the present invention, gateway 16 also features a pre-filtering module 30 which receives the packets before firewall 18, but which is preferably directly connected to protected network 12. Pre-filtering module 30 also preferably receives instructions from firewall 18, concerning packets which are permitted to enter protected network 12. These instructions are more preferably determined by firewall 18 from an analysis of one or more previously received and related packets, such that if a previously received and related packet has been permitted to enter protected network 12, then the current packet should also be permitted to enter protected network 12. Firewall 18 inspects the contents of such packet or packets, and base upon the output of analysis module 24 with rulebase 26, determines whether packets from the corresponding connection should be permitted to enter and/or leave protected network 12 (line 67, Col. 6 and lines 1-4, Col. 7). Alternatively, if the packet is not permitted according to rule base 26, then the packet is optionally dropped (lines 55-56, Col. 5)]. Fink et al. do not expressly disclose the scanning engine and the action of testing and disregarding of packet is associated to the virus. However, Fink et al. disclose the invention is implemented for the purpose of anti-spoofing and any packet(s) that cause violation [i.e., **Alternatively and optionally, even if only the interface is not correct,**

pre-filtering module 30 may determine that the packet represents a violation which should be further inspected by firewall 18 for validity. There are other ways to implement an anti-spoofing method, without including information concerning the interface as part of the stored instructions for pre-filtering module 30, which are also considered to be within the scope of the present invention (lines 39-47, Col. 7)]. Therefore, It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. to have the inspection and filtering of the packet on the virus since one would have been motivated to **provide security by controlling the traffic being passed, thus preventing illegal communication attempts, both within single networks and between connected networks (lines 31-33, Col. 1 in Fink et al.).** Thus, it would have been obvious to modify Fink et al. to obtain the invention as specified in claim 1.

ii. Referring to Claim 2:

As per Claim 2, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose wherein: the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the

virus scanning engine for testing thereof [i.e., Thus, if pre-filtering module 30 determines that the current packet is permitted to enter, then preferably pre-filtering module 30 passes the packet directly through to protected network 12 (lines 17-32, Col. 6). Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determined that the packet represents a violation which should be further inspected by firewall for validity (lines 39-42, Col. 7)].

iii. Referring to Claim 3:

As per Claim 3, Fink et al. disclose a system in accordance with claim 2. In addition, Fink et al. wherein: the virus scanning engine tests the data packets of the second type and forwards those data packet which are tested to not contain a virus to the destination [i.e., Alternatively and optionally, even if only the interface is not correct, pre-filtering module 30 may determined that the packet represents a violation which should be further inspected by firewall for validity (lines 39-42, Col. 7). Gateway 16 operates a firewall 18 for performing packet analysis and packet filtering (lines 33-34, Col. 5). Firewall 18 features a packet filter 22 for performing packet filtration. Packet filter 22 in turn is preferably composed of an analysis module 24 for analyzing packets and a rule base 26 (lines 42-46, Col. 5). Analysis module 24 extracts and compares the contents of the analyzed

packets to the rules in rule base 26. If the result of the comparison is such tat the packet is permitted according to rule base 26, the packet filter 22 permits packet to enter protected network 12 (lines 48-53, Col. 5)].

iv. Referring to Claim 20:

As per Claim 20, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose the firewall drops any received data packet which are tested to be illegal according to firewall rules [i.e., Rule base 26 preferably contains one or more rules which are defined according to the preferences of the system administrator or other controller user (lines 46-48, Col. 5). Alternatively, if the packet is not permitted according to rule base 26, then the packet is optionally dropped (lines 55-56, Col. 5)].

v. Referring to Claim 21:

As per Claim 21, the rejection of Claim 2 is incorporated. In addition, Claim 21 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

vi. Referring to Claim 32:

As per Claim 32, Fink et al. disclose a system in accordance with claim 21. In addition, Fink et al. disclose a packet classification database, coupled to the firewall, which provides information to the firewall which

defines the first and second types of data packets [i.e., **Pre-filtering module 30** also preferably features a **classification engine 38**, including a data processor, for at least partially analyzing the information from the packet and for retrieving information from connection database 32 (lines 4-7, Col. 8). With the help of information and instructions retrieved from database 32 in memory 36, classification engine 38 then analyzes at least a portion of the information in each packet (lines 38-41, Col. 8)];

A virus detection data base, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine [i.e., **Packet filter 22** in turn is preferably composed of an analysis module for analyzing packets and a rule base 26. Rule base 26 preferably contains one or more rules which are defined according to the preferences of the system administrator or other controlling user. Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in the rule base 26 (line 44-50, Col. 5)].

vii. Referring to Claim 41:

As per Claim 41, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a local area network [i.e., **protected network 12 (Fig. 1)**].

viii. Referring to Claim 42:

As per Claim 42, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a personal computer **[i.e., protected node 12 within the protected network 20 (Fig. 1). Hereinafter, the term “network” includes a connection between any two or more computational devices which permits the transmission of data. Hereinafter, the term “computational” device” includes, but not limited to, personal computers (PC) having an operating system (lines 39-44, Col. 3)]**

ix. Referring to Claim 43:

As per Claim 44, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the destination is a second network **[i.e., protected network 12 (Fig. 1)].**

x. Referring to Claim 44:

As per Claim 44, the rejection of Claim 1 is incorporated. In addition, Fink et al. disclose the first network is a wide area network **[i.e., External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5)].**

xi. Referring to Claim 45:

As per Claim 45, the rejection of Claim 44 is incorporated. In addition, Fink et al. disclose the wide area network is the Internet **[i.e., External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5)].**

xii. Referring to Claim 47:

As per Claim 47, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose the virus scanning engine decodes the data packets during determination if the data packets contain a virus [i.e., Gateway 15 operates a firewall 18 for performing packet analysis and packet filtering (lines 33-34, Col. 5). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in the rule base 26 (lines 48-50, Col. 5). In addition, from the rules which are stored in rule base 26, analysis module 24 is able to determine one or more actions which should be associated with each connection. Examples of such actions include, but are not limited to, performing an accounting action in order to count the amount of data in the packet, encrypting/decrypting the packet, performing network address translation (NAT) by rewriting the address fields, and so forth (lines 4-11, Col. 7)].

xiii. Referring to Claim 49:

As per Claim 49, it is a method claim corresponding to the system claim 1. Therefore, it is rejected with the same rationale applied against Claim 1 above.

xiv. Referring to Claim 50:

As per Claim 50, Fink et al. disclose in a communication system including at least a first network coupled to a destination to which

transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall which receives the data packets and the virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus as in Claim 1. In addition, Fink et al. disclose a computer program stored on a storage medium [i.e., **The device comprising: (a) a memory for storing at least one instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)] and the computer program when executed causing the virus scanning engine to execute at least one step of testing the data packets for the presence of a virus [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rules base 26 (lines 48-50, Col. 5)].****

xv. Referring to Claim 51:

As per Claim 51, Fink et al. disclose a computer program in accordance with claim 50. Fink et al. disclose the firewall classifies the received data packets into packets of a first type which cannot contain a virus and second type which can contain a virus and forwards the data packets of the first type to the destination without testing by the virus scanning engine and forwards the data packets of the second type to the virus scanning engine for testing thereof as in Claim 2. In addition, Fink et al. disclose wherein: the computer program when executed causes the virus scanning engine to test the data packets of the second type and causes the virus scanning engine to forward those data packets which are tested to not contain a virus to the destination [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3). Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12. Analysis module 24 extracts and compares the contents of the analyzed packets to the rules in rule base 26. If the result of the comparison is such that**

the packet is permitted according to rule base 26, then packet filter 22 permits the packet to enter protected network 12 (lines 48-53)].

xvi. Referring to Claim 52:

As per Claim 52, the rejection of 50 is incorporated. In addition, Claim 53 encompasses limitations that are similar to those of Claim 1. Therefore, it is rejected with the same rationale applied against Claim 1.

xvii. Referring to Claim 55:

As per Claim 55, the rejection of 50 is incorporated. In addition, Claim 55 encompasses limitations that are similar to those of Claims 20 and 32. Therefore, it is rejected with the same rationale applied against Claims 20 and 32.

6. Claims 4-5, 11-12, 46, 48, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claims 1-3 and 47 above, and further in view of Franczek et al. (U.S. Patent 6,397,335).

i. Referring to Claim 4:

As per Claim 4, Fink et al. disclose a system in accordance with Claim 2. Fink et al. do not expressly disclose the data packets of the first type contain real time data. However, Franczek et al. disclose that stream data can be communicated between the client and server in the network environment **[i.e., Virus-free streams are reconstructed prior to communicating the data to the receiving party. In this way, the**

system is operative when there are multiple data streams defined between a client and a server (lines 20-24, Col. 12)]. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to have the stream data in the packet(s) communicating in the network environment since one would be motivated to **perform virus screening separately on each of a plurality of virtual channels included in an interactive session (lines 17-19, Col. 12 in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 4.

ii. Referring to Claim 5:

As per Claim 5, the rejection of Claim 3 is incorporated. In addition, Claim 5 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4 above.

iii. Referring to Claim 11:

As per Claim 11, Fink et al. disclose a system in accordance with claim 2. Fink et al. do not expressly disclose the remaining limitation of the claim. However, Franczek et al. disclose a buffer **[i.e., a Preferably, each virus-screening processor has an associated memory device**

to store at least two packets (lines 13-14, Col. 5)] which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus [i.e., **Alternatively the virus screening can be performed in-line by partitioning the file into small blocks of data, screening each block of data, and communicating each virus-free block data upon being screened (lines 64-67, Col. 11)]**. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to have a storage buffer for a large packet(s) to be inspected since one would be motivated to **examine one more succeeding blocks since a virus signature could extend over several blocks of data (lines 3-5, Col. 12 in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 11.

iv. Referring to Claim 12:

As per Claim 12, the rejection of Claim 3 is incorporated. In addition, Claim 12 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

v. Referring to Claim 46:

As per Claim 46, Fink et al. disclose a system in accordance with claim 1. In addition, Fink et al. disclose wherein: the first network is the Internet as in Claim 44 and the gateway is linked between the external network and destination. Fink et al. do not expressly disclose coupling to an Internet service provider and a modem coupled to the Internet service provider and one of local area or personal computer coupled to the modem. However, Franczek et al. disclose a personal computer linked to the internet service provider through the modem [i.e., **A user computer 400 having a modem 402 communicates with a modem 404 associated with an internet service providers 406 (lines 51-53, Co. 12). Other connection means such as an integrated service digital network (ISDN), a digital subscriber line (DSL), or cellular data can be used to link the user computer 400 to the internet service provider 406 (lines 55-58, Col. 12)]]. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to integrate the gateway with the typical internet dial-up service setup in the network environment since one would be motivated to have **a service provider may subscribe to the virus screening service to protect its users from computer viruses by screening its transmitted computer data****

(lines 36-39, Col. 3 in Franczek et al.). Therefore, it would have been obvious to modify Fink et al. with Franczek et al. to obtain the invention as specified in claim 46.

vi. Referring to Claim 48:

As per Claim 48, Fink et al. disclose a system in accordance with claim 47. Fink et al. does not expressly disclose that the virus scanning engine functions as a proxy for a destination processor which receives the data packets. However, Franczek et al. disclose the virus screening processors can function as a proxy server [i.e., **The herein-described virus-screening processors can provide or assist in providing a proxy server or a functional equivalent of a proxy server (lines 3-5, Col. 5)]**. Fink et al. and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Franczek et al. to have the various components altogether within the gateway functioning as a proxy server in the network environment since one would be motivated to have **the virus-screening processor can create and communicate modified protocol-specific information such as a number of packets to be received, error detection and correction information, and packet serial numbers (lines 9-12, Col.5 in in Franczek et al.)**. Therefore, it would have been obvious to modify

Fink et al. with Franczek et al. to obtain the invention as specified in claim 48.

vii. Referring to Claim 53:

As per Claim 53, the rejection of 51 is incorporated. In addition, Claim 53 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale applied against Claim 4.

7. Claims 13-14, 22-23, 27, 33, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 4-5 and 11-12 above.

i. Referring to Claim 13:

As per Claim 13, the rejection of Claim 4 is incorporated. In addition, Claim 13 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

ii. Referring to Claim 14:

As per Claim 14, the rejection of Claim 5 is incorporated. In addition, Claim 14 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

iii. Referring to Claim 22:

As per Claim 22, the rejection of Claim 4 is incorporated. In addition, Claim 22 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iv. Referring to Claim 23:

As per Claim 23, the rejection of Claim 5 is incorporated. In addition, Claim 23 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

v. Referring to Claim 27:

As per Claim 27, the rejection of Claim 12 is incorporated. In addition, Claim 27 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

vi. Referring to Claim 33:

As per Claim 33, the rejection of Claim 4 is incorporated. In addition, Claim 33 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

vii. Referring to Claim 36:

As per Claim 36, the rejection of Claim 11 is incorporated. In addition, Claim 36 encompasses limitations that are similar to those of Claim 32.

Therefore, it is rejected with the same rationale applied against Claim 32 above.

8. Claims 28 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 13-14 above.

i. Referring to Claim 28:

As per Claim 28, the rejection of Claim 14 is incorporated. In addition, Claim 28 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 37:

As per Claim 37, the rejection of Claim 13 is incorporated. In addition, Claim 37 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

9. Claims 6-8 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claims 1-3 and 50 above, and further in view of Lyle (U.S. Patent 6,886,012).

i. Referring to Claim 6:

As per Claim 6, Fink et al. disclose a system in accordance with claim 1. Fink et al. do not expressly disclose wherein: the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which, in response to the alert, stops reception of a data stream containing the data packets. However, Lyle discloses that an alert message can be sent to various components in order to prevent them participating in flowing around the data containing malicious code [i.e., **In one embodiment, as described above, the responsive action for one or more types of incident may include sending an alert, such as by activating a pager and/or sending an e-mail message to alert a network security administrator to the fact that an alert condition is present, or sending an appropriate message to a router or switch to stop a malicious flow of network traffic (lines 28-34, Col. 14)].** Fink et al. and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to **share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2).**

Therefore, it would have been obvious to modify Fink et al. with Lyle to obtain the invention as specified in claim 6.

ii. Referring to Claim 7:

As per Claim 7, the rejection of Claim 2 is incorporated. In addition, Claim 7 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

iii. Referring to Claim 8:

As per Claim 8, the rejection of Claim 3 is incorporated. In addition, Claim 8 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above.

iv. Referring to Claim 54:

As per Claim 54, the rejection of 50 is incorporated. Claim 54 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale applied against Claim 6 above. In addition, Fink disclose the computer program [i.e., **The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3).**].

10. Claims 24-25 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Lyle (U.S. Patent 6,886,012) as applied to claims 6-7 above.

i. Referring to Claim 24:

As per Claim 24, the rejection of Claim 6 is incorporated. In addition, Claim 24 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 25:

As per Claim 25, the rejection of Claim 7 is incorporated. In addition, Claim 25 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iii. Referring to Claim 34:

As per Claim 34, the rejection of Claim 7 is incorporated. In addition, Claim 34 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

11. Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) as applied to claim 1 above, and further in view of Radatti (U.S. Patent 6,721,424).

i. Referring to Claim 40:

As per Claim 40, Fink et al. disclose a system in accordance with claim 1. Fink et al. do not expressly disclose wherein: the virus scanning engine, upon detection of a virus in the data packets, also alerts the destination that a virus has been detected. However, Radatti discloses an alert message is sent to notify the destination user of the virus presence in the data [i.e., **The gateway server 20 issues an appropriate alert or otherwise takes action to prevent transmission of the virus to the destination of the data transfer. For example, the gateway server 20 may issue a message to the destination user station notifying the user that an incoming data transfer was determined to contain a virus (lines 30-36, Col. 4)**]. Fink et al. and Radatti are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. with Radatti to have the alert message generated and sent to the destination upon detecting the malicious code since one would be motivated to **take action to prevent transmission of the virus to the destination of the data transfer (lines 31-32, Col. 4 in Radatti)**. Therefore, it would have been obvious to modify Fink et al. with Radatti to obtain the invention as specified in claim 40.

12. Claims 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 4-5 above, and further in view of Lyle (U.S. Patent 6,886,012).

i. Referring to Claim 9:

As per Claim 9, Fink et al. and Franczek et al. disclose a system in accordance with claim 4. Fink et al. and Franczek et al. do not expressly disclose wherein: the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which in response to the alert stops reception of a data stream containing the data packets. However, Lyle discloses that an alert message can be sent to various components in order to prevent them participating in flowing around the data containing malicious code **[i.e., In one embodiment, as described above, the responsive action for one or more types of incident may include sending an alert, such as by activating a pager and/or sending an e-mail message to alert a network security administrator to the fact that an alert condition is present, or sending an appropriate message to a router or switch to stop a malicious flow of network traffic (lines 28-34, Col. 14)]**. Fink et al., Franczek et al., and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data

communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Franczek et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to **share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2 in Lyle)**. Therefore, it would have been obvious to modify Fink et al. and Franczek et al. with Lyle to obtain the invention as specified in claim 9.

ii. Referring to Claim 10:

As per Claim 10, the rejection of Claim 5 is incorporated. In addition, Claim 10 encompasses limitations that are similar to those of Claim 9. Therefore, it is rejected with the same rationale applied against Claim 9 above.

13. Claims 18-19, 26, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Franczek et al. (U.S. Patent 6,397,335), and Lyle (U.S. Patent 6,886,012) as applied to claims 9-10 above.

i. Referring to Claim 18:

As per Claim 18, the rejection of Claim 9 is incorporated. In addition, Claim 18 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

ii. Referring to Claim 19:

As per Claim 19, the rejection of Claim 10 is incorporated. In addition, Claim 19 encompasses limitations that are similar to those of Claim 11. Therefore, it is rejected with the same rationale applied against Claim 11 above.

iii. Referring to Claim 26:

As per Claim 26, the rejection of Claim 9 is incorporated. In addition, Claim 26 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iv. Referring to Claim 35:

As per Claim 35, the rejection of Claim 9 is incorporated. In addition, Claim 35 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

14. Claims 31 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Franczek et al. (U.S. Patent 6,397,335), and Lyle (U.S. Patent 6,886,012) as applied to claim 18 above.

i. Referring to Claim 31:

As per Claim 31, the rejection of Claim 18 is incorporated. In addition, Claim 31 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 39:

As per Claim 39, the rejection of Claim 18 is incorporated. In addition, Claim 39 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale applied against Claim 32 above.

15. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and Lyle (U.S. Patent 6,886,012) as applied to claims 6-8 above, and further in view of Franczek et al. (U.S. Patent 6,397,335).

i. Referring to Claim 15:

As per Claim 15, Fink et al. and Lyle disclose a system in accordance with claim 6. Fink et al. and Lyle do not expressly disclose the remaining limitation of the claim. However, Franczek et al. disclose a buffer [i.e., a **Preferably, each virus-screening processor has an associated**

memory device to store at least two packets (lines 13-14, Col. 5)] which stores the data packets of the second type while the virus scanning engine is processing the data packets of the second type to detect a virus **[i.e., Alternatively the virus screening can be performed in-line by partitioning the file into small blocks of data, screening each block of data, and communicating each virus-free block data upon being screened (lines 64-67, Col. 11)]**. Fink et al., Lyle, and Franczek et al. are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al. and Lyle with Franczek et al. to have a storage buffer for a large packet(s) to be inspected since one would be motivated to **examine one more succeeding blocks since a virus signature could extend over several blocks of data (lines 3-5, Col. 12 in Franczek et al.)**. Therefore, it would have been obvious to modify Fink et al. and Lyle with Franczek et al. to obtain the invention as specified in claim 15.

ii. Referring to Claim 16:

As per Claim 16, the rejection of Claim 7 is incorporated. In addition, Claim 16 encompasses limitations that are similar to those of Claim 15. Therefore, it is rejected with the same rationale applied against Claim 15 above.

iii. Referring to Claim 17:

As per Claim 17, the rejection of Claim 8 is incorporated. In addition, Claim 17 encompasses limitations that are similar to those of Claim 15. Therefore, it is rejected with the same rationale applied against Claim 15 above.

16. Claims 29-30, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Lyle (U.S. Patent 6,886,012), and Franczek et al. (U.S. Patent 6,397,335) as applied to claims 15-16 above.

i. Referring to Claim 29:

As per Claim 29, the rejection of Claim 15 is incorporated. In addition, Claim 29 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

ii. Referring to Claim 30:

As per Claim 30, the rejection of Claim 16 is incorporated. In addition, Claim 30 encompasses limitations that are similar to those of Claim 20. Therefore, it is rejected with the same rationale applied against Claim 20 above.

iii. Referring to Claim 38:

As per Claim 38, the rejection of Claim 16 is incorporated. In addition, Claim 38 encompasses limitations that are similar to those of Claim 32.

Therefore, it is rejected with the same rationale applied against Claim 32 above.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Baehr et al. (U.S. Patent 5,878,231) disclose a system for screening data packets transmitted between a network to be protected, such as a private network, and another network, such as a public network. The proxy network is isolated from the private network and the packet are received at the screen are filtered based upon their contents, state information and other criteria. Encryption and decryption may also automatically be executed on certain data packets. The system includes a fragmentator 660 as to fragment packets that are larger than a predefined maximum transmission unit, and use the fragmentation cache for implementation of fragmentation and reconstruction of packets. In addition, the module in Fig. 9 includes a packet inspector 600 with a process 602-606 for each network interfaces; and engine 610 with rule 620; actions 630 and a log file storage 640, and a packet state table 650.
- b. Kim (U.S. Pub. 2002/0069356) discloses a networking system with an integrated security gateway for integrating virtual private networking, firewall, and network monitoring functions. Fig. 6 shows a functional block

diagram of an integrated security gateway in Fig. 4. The gateway also includes a packet duplicating module 601 and an inspection engine 610, for network interfaces 621-624, rule storage 630, a session table 650 and an action module 660. The action module 660 includes a number of modules, e.g., an encryption module 661, a decryption 662, a URL/content filtering module 663 and NAT module 664. The URL/contents filtering module 663 performs typical URL/contents filtering functions to prevent access to a predetermined group of URL and to drop the packet containing noxious contents.

- c. Ylonen et al. (U.S. Pub. 2003/0110379) disclose a method and apparatuses are disclosed for handling digital data packets. The objective is achieved by implementing packet-level processing in the operating system kernel of a firewall computer, by setting up at least one protocol-specific application gateway somewhere else than in the operating system kernel of the firewall computer, and by instructing the packet-level processing process to recognize packets associated with the protocol that the protocol-specific application gateway handles and to direct the recognized packets to the application gateway. According to the principle of dynamic changing the application gateway part may respond to the arrival of certain ftp control channel signalling by asking the packet processor part to change its redirecting strategy so that also the ftp data channel packets will be redirected, for example in order to check for

viruses that might come embedded in a file transferred over the ftp data channel.

- d. Makinson et al. (U.S. Pub. 2003/0021280) disclose a network bridge (14) has an associated malware scanner (16) that serves to concatenate portions of a data file from within data packets intercepted by the network bridge (14) and then scan the data file concerned before the data file is forwarded to its intended recipient by the network bridge (14). The processing performed by the central processing unit may effectively carry out malware scanning by comparing a received data file against a collection of malware defining data, such as virus definition data. This virus definition data, and an associated scanner engine program, may be automatically updated from a central source, such as an anti-virus providers FTP server, with the scanner 16 making an internet connection via a detected gateway to download updated virus definition data or an updated scanner engine program.
- e. Grosse (U.S. Patent 6,205,551) discloses a technique for determining whether particular clients within a computer network are universally configured in accordance with the desired network security features of the computer network. A probe is randomly inserted within incoming files, e.g., at a firewall in the computer network. The probe is configured as a function of a particular execution task, e.g. a known virus, such that in a

Art Unit: 2135

properly configured client the probe will not execute and the firewall does not detect a security breach.


18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Jul. 20, 2005


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135